

Exhibit A

From: lockardv@gtlaw.com
To: [Layne Hilton](#)
Cc: valpec@kirtlandpackard.com; DECValsartan@btlaw.com
Subject: RE: In re Valsartan, Losartan, Irbesartan - Marker Group Data Breach
Date: Friday, February 25, 2022 1:42:58 PM
Attachments: [Marker Valsartan Excel.xlsx](#)
[Marker Data Event Letter.pdf](#)

Layne,

If you have the letter from other litigations then you likely have the same one I received, which appeared to be a form letter, not specific to any litigation. But I have attached that letter here for you, which was the first notice we received of the event. Plaintiffs' counsel were likely aware before we were, given some of the valsartan plaintiff firms had filed a class action against Marker as early as January. In any event, the letter specifically indicates that Marker was providing notice directly to the individuals whose information was impacted, so your clients should have gotten notice directly from Marker. Marker provided the attached excel which lists 88 individuals who appear to be valsartan plaintiffs, and my understanding is that these are the only valsartan plaintiffs impacted.

The Marker event has impacted a number of litigations our firm is involved in, so we have engaged our firm's information security team who has been working to understand the scope and nature of Marker's event and obtain assurances about tightened security protocols. Again, however, I think the best approach is to try to set a call with Marker so that we can get you the information you require directly from them, since they are much better suited to describe what happened and how they are addressing it. Let me know when you would be available for that.

Thanks, Victoria

Victoria Davis Lockard
Shareholder
Greenberg Traurig, LLP | 3333 Piedmont Road NE | Suite 2500 | Atlanta, GA 30305
Tel 678.553.2103 | Fax 678-553-2104
lockardv@gtlaw.com | www.gtlaw.com



From: Layne Hilton <l.hilton@kanner-law.com>
Sent: Friday, February 25, 2022 10:37 AM
To: Lockard, Victoria D. (Shld-ATL-LT) <lockardv@gtlaw.com>; DECValsartan@btlaw.com
Cc: valpec@kirtlandpackard.com
Subject: RE: In re Valsartan, Losartan, Irbesartan - Marker Group Data Breach

Victoria:

In this litigation the Plaintiffs do NOT have any direct contractual relationship with Marker and have

not otherwise affirmatively provided any of their clients' PHI or confidential information to Marker for collection of records. We merely have "opposing counsel" credentials which permit us to purchase medical records previously retrieved by Defendants on an ad hoc basis, and have provided our own credit card information for such purchases.

While we will surely make inquiries with Marker, we have seen that in other litigations, the defense attorneys have provided the Plaintiffs' Counsel with correspondence from Marker's attorneys that they received which further elaborate on the scope and/or extent of the breach.

Can you confirm that no Defendants' Counsel in this litigation (and not your firm, Greenberg Traurig) has received a letter from the Marker Group's attorneys regarding the data breach and its impact on any Valsartan, Losartan or Irbesartan Plaintiff?

Thanks,

Layne

From: lockardv@gtlaw.com <lockardv@gtlaw.com>

Sent: Wednesday, February 23, 2022 2:49 PM

To: Layne Hilton <l.hilton@kanner-law.com>; DECValsartan@btlaw.com

Cc: valpec@kirtlandpackard.com

Subject: RE: In re Valsartan, Losartan, Irbesartan - Marker Group Data Breach

Layne,

Our firm only just learned of this issue with this third-party vendor ourselves recently (which impacts litigations other than just valsartan) and are in the process of gathering information and trying to understand the scope of the event from Marker and understand what steps they have instituted. It is my understanding that Plaintiffs are also using Marker and would have direct agreements with Marker, and that Marker was in the process of issuing notices to Plaintiffs as well as certain regulatory agencies. So I think you are certainly within right to ask Marker for the information you need from them if you have not yet received it. My suggestion is that we discuss by phone and then set a joint call with Marker if necessary to gather the additional information you request below. Let me know your thoughts on that.

Victoria Davis Lockard

Shareholder

Greenberg Traurig, LLP | 3333 Piedmont Road NE | Suite 2500 | Atlanta, GA 30305

Tel 678.553.2103 | Fax 678-553-2104

lockardv@gtlaw.com | www.gtlaw.com



From: Layne Hilton <l.hilton@kanner-law.com>

Sent: Wednesday, February 23, 2022 3:20 PM

To: 'DECValsartan@btlaw.com' <DECValsartan@btlaw.com>

Cc: valpec@kirtlandpackard.com

Subject: [EXTERNAL]RE: In re Valsartan, Losartan, Irbesartan - Marker Group Data Breach

EXTERNAL TO GT

Counsel:

Following up on the below. We have also realized that to the extent any attorneys/firms provided the Marker Group with logins and passwords, credit cards, or other payment methods, this information has also been potentially impacted by the data breach.

Plaintiffs ask for an update about this data breach by tomorrow.

Best,

Layne

From: Layne Hilton

Sent: Wednesday, February 16, 2022 10:26 AM

To: 'DECValsartan@btlaw.com' <DECValsartan@btlaw.com>

Cc: valpec@kirtlandpackard.com

Subject: In re Valsartan, Losartan, Irbesartan - Marker Group Data Breach

Counsel:

Plaintiffs have just become aware of the data-breach that occurred at the Marker Group, the data vendor utilized by Defendants for the collection and retention of medical records in this case. At Defendants' request and facilitation, the Marker Group has retained records containing the following pieces of highly sensitive information about Plaintiffs contained with the Plaintiffs' Fact Sheet ("PFS), such as but not limited to: social security numbers, addresses for the 10 years, maiden names, previous lawsuits, and dates of birth. Moreover, the medical records retrieved and maintained by the Marker Group contain medical treatment and diagnosis information (collectively considered "protected health information" or "PHI").

Plaintiffs are extremely concerned they had to learn of the extensive Marker Group breach from the news and were not provided notification by the Defendants themselves. Indeed, the only communications Plaintiffs have received related to the Marker Group indicate that despite this data breach, the Defendants continue to use the Marker Group to retrieve and maintain highly protected

PHI and medical records.

Plaintiffs ask that Defendants confirm the following:

- The date of the purported data breach;
- The date upon which the data breach was discovered by the Marker Group;
- The date upon which the data breach was communicated to Defendants;
- Whether any documentation related to any Plaintiff in the Valsartan, Losartan or Irbesartan litigation was implicated in this data breach;
- The identity of any such Plaintiff whose data was implicated in this data breach;
- The documentation implicated for those Plaintiffs in said data breach;
- Whether Marker Group and/or Defendants have received reports of actual or attempted misuse of any of this information;
- Whether the Marker Group intends to send direct notifications to individuals whose information was implicated in the data breach; and
- The efforts Defendants and/or the Marker Group have taken in order to further protect the PHI and other associated data contained within Plaintiffs' Fact Sheets and associated medical records in order further safeguard Plaintiffs' information contained in PFSs and/or the documents being retrieved and maintained on their system.

We ask for confirmation of the above information as soon as possible.

Best,

Layne

Layne Hilton
Kanner & Whiteley, L.L.C.
701 Camp Street
New Orleans, LA 70130
(504) 524-5777 voice
(504) 524-5763 fax
www.kanner-law.com

THIS EMAIL MESSAGE IS FOR THE SOLE USE OF THE INTENDED RECIPIENT(S) AND MAY CONTAIN CONFIDENTIAL AND PRIVILEGED INFORMATION. IF YOU ARE NOT THE INTENDED RECIPIENT, PLEASE CONTACT THE SENDER BY REPLY EMAIL AND DESTROY ALL COPIES OF THE ORIGINAL MESSAGE. _____

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly

prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

CONFIDENTIALITY NOTICE: This email and any attachments are for the exclusive and confidential use of the intended recipient. If you are not the intended recipient, please do not read, distribute or take action in reliance upon this message. If you have received this in error, please notify us immediately by return email and promptly delete this message and its attachments from your computer system. We do not waive attorney-client or work product privilege by the transmission of this message.

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at postmaster@gtlaw.com, and do not use or disseminate the information.

February 2, 2022

VIA ELECTRONIC MAIL

Victoria Lockard
Greenberg Traurig
lockardv@gtlaw.com

Subject: Notice of Data Event

The Marker Group, Inc. (“Marker Group”) writes to inform you of a recent data security event. This letter contains information about the event and our response. Please review the below for more details on this incident and the steps Marker Group is taking.

WHAT HAPPENED?

On September 3, 2021, Marker Group learned that certain systems in its computing environment had become encrypted due to “ransomware” deployed by an unknown actor. Upon discovery of the event, Marker Group engaged cybersecurity specialists to conduct a thorough investigation into the cause and scope of the incident to determine what information may have been accessed by the unknown actor.

In response to the event, all critical impacted systems were identified through thorough forensic analysis and any indicators of compromise were subjected to malware analysis and incorporated into the Carbon Black endpoint detection and response software, which is monitored around the clock for signs or suspicious activity or behavior. Since the completion of containment and remediation, no malicious alerts have been generated in connection with the event.

Through the investigation, Marker Group determined that an unknown actor gained access to certain Marker Group systems, which stored data. Although temporarily taken offline as a precaution following the discovery of the event, the databases used by Marker Group clients were not impacted, and no files were lost or altered in this event. However, while the investigation did not identify any evidence that files were taken, it could not affirmatively rule out the potential that the unauthorized actor took files from Marker Group systems. Importantly, there are no indications that any Marker Group data has been misused or will be released to the public.

Unfortunately, the investigation determined that the impacted systems held files with sensitive information related to plaintiffs/parties in a litigation matter in which Greenberg Traurig is involved. Although we do not have any indication of misuse of personal information at this time, we are providing this notification to you out of an abundance of caution.

WHAT MARKER GROUP IS DOING

Marker Group's computing environment has been restored to a fully operational status with the assistance of an industry-leading firm with superior digital forensics and incident response experience. The response to this event was conducted with industry best practices for matters involving technical security incidents.

Following the event, Marker Group installed new operating systems and sealed hard drives across the environment. All legacy hard drives were fully decommissioned and removed from the network. The Marker Group Active Directory was reverted to a version from 60 days prior to the first indicator of compromise. In addition to its existing antivirus and endpoint protection tools, Marker Group has deployed Carbon Black endpoint detection and response software across the environment. Carbon Black is actively

Greenberg Traurig
February 2, 2022

monitored around the clock by a third-party security operations center. The latest alert in the Carbon Black console occurred on September 3, 2021. No subsequent malicious activity has been identified.

In addition, Marker Group rebuilt its email server from the ground up without utilizing the existing stores or configuration. No backend systems or user workstations were reintroduced into the environment unless wiped and rebuilt or subjected to thorough malware analysis and active monitoring. All machines in the environment are scanned via Symantec Endpoint Protection on a daily basis. Marker Group has updated all administrative and system passwords, hardened its firewall rules, enhanced information security policies and procedures, and is implementing additional workforce training to reduce the likelihood of a similar future event.

At this time, all impacted or at-risk systems have been removed from the Marker Group environment and decommissioned, cleaned and rebuilt from scratch, and/or are under 24/7 monitoring by the third-party forensic firm. The containment and remediation work performed by the forensic team, paired with the lack of Carbon Black alerts related to the ransomware event since the conclusion of Marker Group's containment effort, gives sufficient confidence that the threat actor has been expelled from the environment. Marker Group has taken significant measures to increase the security of its systems and further protect its clients and their data.

Marker Group is providing written notice of this incident to individuals whose sensitive information was located within the potentially impacted systems and offering these individuals complimentary credit monitoring. Notice will be provided to the potentially impacted individuals by way of a letter in substantially the same form as attached **Exhibit A**. Marker Group is also providing notification of this incident to regulatory authorities as required under applicable laws.

CLOSING COMMENTS

Marker Group sincerely apologizes for any inconvenience or frustration this may have caused. Marker Group is adding additional layers of control and will continue to seek improvements. To this end, we are reviewing our vendors, processes, and systems with an eye toward reducing risks to avoid a similar incident in the future.

If you have any questions about this letter, please contact Marker Group at 1-877-934-2721 or IRT@marker-group.com.

Sincerely,



Melissa Marker Ruzicka
Vice President
The Marker Group

[Enclosures: **Exhibit A**]

Exhibit A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Notice of Data <<Variable 1>>

The Marker Group is writing to make you aware of an incident that may affect the privacy of some of your information. Marker Group provides litigation support services to law firms in the United States, including hosting data for law firms to share and access during the course of a lawsuit. You are receiving this letter because you are associated with a litigation matter in which your personal information was involved. This letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On September 3, 2021, Marker Group discovered suspicious activity on certain systems in our computer network. As a result, we immediately worked to secure our environment and, with the assistance of third-party computer specialists, launched an investigation to determine the nature and scope of the activity. On or about September 10, 2021, the investigation determined that certain files on our systems may have been accessed by an unknown, unauthorized third party. We immediately began a review of the potentially impacted files and our internal systems to identify the information involved and to whom it related. Unfortunately, on December 13, 2021, we determined that certain files containing your information could have been accessed during the event. While there is no indication that your specific information was or will be misused, we are notifying all potentially impacted individuals out of an abundance of caution.

What Information was Involved? Our investigation determined that the following types of information related to you may have been impacted: name, date of birth, Social Security number, and/or various types of medical records containing treatment and insurance information.

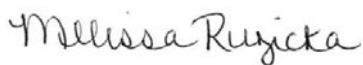
What we are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<Insert 12 months or 24 months>> provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Individuals who wish to receive these services must enroll by following the enrollment instructions in the enclosed “*Steps You Can Take to Help Protect Your Information.*”

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your Explanation of Benefits and free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed “*Steps You Can Take to Help Protect Your Information.*”

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 855-604-1716 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Melissa Ruzicka".

Melissa Marker Ruzicka
Vice President
The Marker Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain << Insert 12 months or 24 months >> of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately [0] Rhode Island residents impacted by this incident.